Risk Assessment: Approach to enhance Network Security

Nwagu, Chikezie Kenneth, Omankwu, Obinnaya Chinecherem, Okonkwo, Obikwelu Raphael

[1]Computer Science Department, Nnamdi Azikiwe University Awka Anambra State, Nigeria.
Nwaguchikeziekenneth@hotmail.com

[2]Computer Science Department, Michael Okpara University of Agriculture Umudike Umuahia, Abia State, Nigeria.
Saintbeloved@yahoo.com

[3]Computer Science Department, Nnamdi Azikiwe University Awka Anambra State, Nigeria.
Oobi2971@yahoo.com

Abstract
This research work x-rays the indispensability of continuous risk assessment on data and communication devices, to ensure that full business uptime is assured and to minimize, if not completely eradicate downtime caused by “unwanted elements of the society” ranging from hackers, invaders, network attackers to cyber terrorists. Considering high-cost of downtime and its huge business negative impact, it becomes extremely necessary and critical to proactively monitor, protect and defend your business and organization by ensuring prompt and regular Risk assessment of the data and communication devices which forms the digital walls of the organization. The work also briefly highlights the methodologies used, methodically discusses core risk assessment processes, common existing network architecture and its main vulnerabilities, proposed network architecture and its risk assessment integration(Proof), highlights the strengths of the proposed architecture in the face of present day business threats and opportunities and finally emphasizes importance of consistent communication and consultation of stakeholders and Original Equipment Manufacturers (OEMs)
Keywords- Risks,Risk Assessment,Network Architecture,vulnerabilities,Opportunities.

I. METHODOLOGY

In the course of this work, some other methodologies such as Object Oriented Analysis and Design Methodologies (OOADM), Incremental/Evolutionary Methodologies etc. were considered and finally adopted Structured System Analysis and Design Method(SSADM), Dynamic System Development Method (DSDM) and Spiral Methodologies.

Reasons for the adoption are their direct applicability and features among which are respectively as follow:
For SSADM,

- Intensive users involvement
- Clear and easily understandable documentation
- Process is Procedural

For DSDM

- Focuses on Business need and delivers on time
- Communicate continuously and clearly without compromising quality

For Spiral

- Risk driven and keeps track of risk patterns in a project.
- Iterative and incremental

All these features are used to analyze common existing network architectures with the primary aim of:

- Identifying bottlenecks and Problems thereof.
- Investigating areas of improvement
- And proffering solutions to the system(Proposed Network Architecture)

II RISKS AND RISK ASSESSMENT

If you don’t assess your data and communication devices, definitely someone else would. And this will invariably leave your organization at the mercy of the attackers – attackers are ill-winds that blow no man any good.In fact, in most cases, organizations are shutdown, monies are lost and the image of the company is battered and left in doubt for the public as data integrity, confidentiality and availability are not assured of.

Risks, contrary to earlier notion, are both positive and negative. Therefore Risk, as adapted from Stoneburner, G., Goguen, A. & Feringa, A. (2002, July), is net negative or positive effect of exercise of vulnerabilities or opportunities which can be exploited, enhanced, shared, transferred, or even accepted.

However, this work focuses on negative risks (vulnerabilities) which can be intentionally exploited or accidentally triggered. Subsequent publication which is part of the entire work, will anatomize risks as opportunities which are positive.

Risk Assessment, as a critical part of risk management, is made of many core processes (which the steps depicted in figure 3 and further explained) such as:

- Risk identification: This allows individuals to identify risks so that the stakeholders will be in the know of potential threats or opportunities inherent in the devices. It is pertinent to start this stage as early as possible and should be repeated frequently.

- Risk analysis and Prioritization: Risk analysis transforms the estimates or data about specific risks that developed during risk identification into a consistent form that can be used to make decisions around prioritization. Risk prioritization enables operations to commit resources to manage the most important or worst risks.
- Integration of Risk registers: This assures that risks (both low and high priority ones) are tracked and monitored through the entire process. In the course of the initial process of Risk assessment, all low-priority risks are kept in the register and while during subsequent risk assessments, the content is updated after the content is assessed, in addition to the entire assessment. As a core part of process and result, contains lists of identified risks, root causes of risks, lists of potential responses, risk owners, symptoms and warning signs, relative rating or priority list. These are risks for additional analysis and responses, and a watch list which is a list of low-priority risks under close watch and monitoring.
- Communication and Consultation: Communication is key is risk assessment. There should be steady and consistent communication/consultation among stakeholders within the organization as everyone is practically involved and outside, especially to Original Equipment Manufacturers (OEMs). In addition, the stakeholders can utilize all their communication channels (Calls, Emails, via Technical Account Managers (TAM), Portal etc.) to the OEMs. This ensures speedy and reliable responses which further assist organizations to strategically align with industry best practices and proactively avoid negative risks.

III. RISK ASSESSMENT KEY STEPS

The Principal steps undertaken in order to thoroughly assess risks associated with ICT systems are:

Step 1 – System/Device Characterization
Step 2 - Vulnerability Identification
Step 3 - Threat Identification
Step 4 - Control Analysis
Step 5 - Likelihood Determination
Step 6 - Impact Analysis and Integration of Risk register
Step 7 - Risk Determination
Step 8 - Control Recommendations
Step 9 - Assessment Documentation and Updating Risk Register

Depending on the level of organizations risk awareness and maturity, steps 2 to 6 can be carried out concurrently after completing step 1.And throughout the entire processes and steps ,there is consistent two-way communication and consultation among stakeholders including OEMs.This is key to ensure successful and seamless risk assessment processes integration into organizational daily operational routines

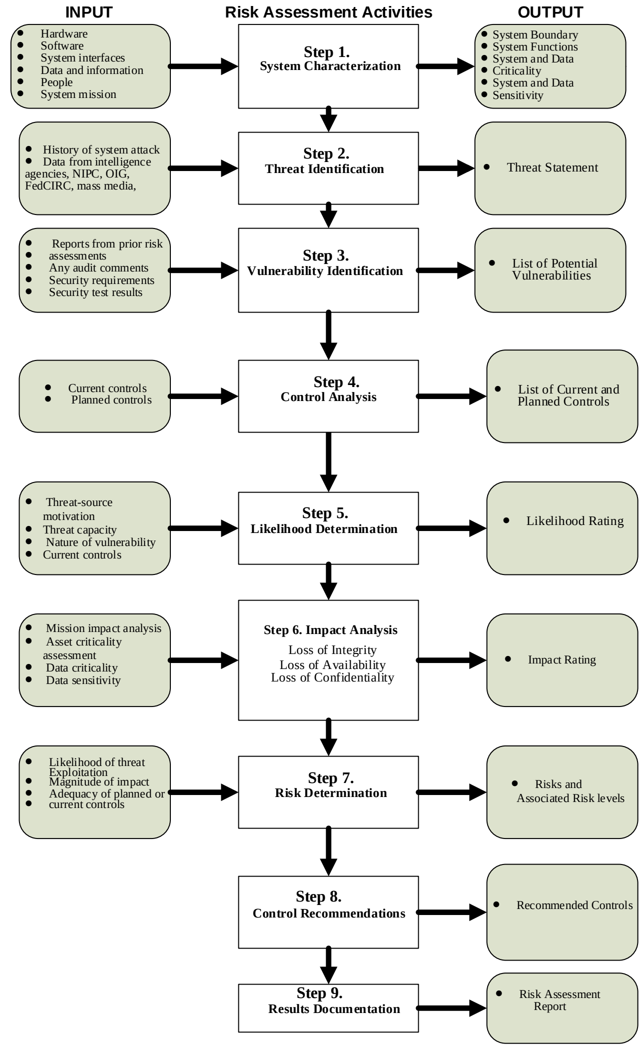

Figure 3: Risk Assessment Process *(adapted from stoneburner et al.)*

Step 1 – Device/System Characterization:
The first step, is basically to define the scope of ICT systems, be it data and communication devices, hardware, software or as your organization need directs. This would assist the stakeholders to establish clear category as outputs at this step based on functionality, criticality and /or sensitivity of the devices/systems. With these, it will be essentially easy to define the risk, its priority and of course, assign appropriate resource which would help to mitigate the identified risks completely at this stage or reduce it to acceptable level which would immediately be kept in the risk register for close monitoring and watch in the subsequent risk assessments. If this happens, would automatically jump the process to step 7 which keeps the end in sight for the entire processes.

Step 2 - Vulnerability Identification
This is principally looking at the existing documentations (risk assessment etc.) and records (audits, continuous quality/process improvement etc.) and studying them, so as to

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

come up with list of vulnerabilities and /or potential vulnerabilities associated with respective devices/ICT systems.

Step 3 - Threat Identification
This involves studying history of attacks and possibly their trend. Accessing and leveraging on similar information from other organizations would be an added advantage as all known threats and their respective sources would reflect on the threat statement. With this broader coverage of threat statement, the risk assessment core processes would be on the lookout for them and mitigating plan proactively put place to ensure no exercise of those threats by the threat sources.

Step 4 - Control Analysis
Having established the systems boundary, possible vulnerabilities identified and threat statement clearly written, it becomes important to analyze existing controls and their respective efficacies and potencies against them(identified vulnerabilities and threat-sources).With these, list of existing current controls would be written and their inadequacies bridged as planned(proposed) controls.

Step 5 - Likelihood Determination
At this stage, threat-source motivation should have been known and put into consideration, nature of the vulnerability and of course, threat capacity if successfully exercised, then likelihood rating could be determined. Likelihood rating is simply the probability that identified vulnerabilities can be exercised successfully by threat-sources. To determine the likelihood involves examining threat-source motivation and capability, type of vulnerability involved and effectiveness of existing controls. Hence the likelihood that a particular potential system weakness could be exercised by a given threat-source is then categorize as ***high or low***. However in most cases, organizations go a little deeper and categorize it as ***high, medium, or low*** depending on the anticipated severity.
It is High when the threats are likely exploitable and the threat source is attracted, very motivated and highly capable to initiate it. However the existing controls are ineffective and insufficient to prevent exercise of the vulnerability thereof.
It is Medium when threats are highly exploitable, the threat source attracted, very motivated and highly capable. However the existing controls may prevent exercise of the vulnerability.
It is low when the threats are not likely exploitable, threat source is not attracted and lacks motivation and capability to initiate the attack. This is mainly due to the existing controls which are sufficient to prevent the exercise of the vulnerability.

Step 6 - Impact Analysis and Integration of Risk register.
This is one of the critical steps of risk assessment processes as the probable adverse impact of successful exercise of the vulnerable is determined and measured for negative risks and optimal benefits/full utilization of the ICT systems is also determined for positive risks to justify for stakeholders especially senior management team the decision taken as regards to likely return on investment (ROI). Integration of Risk register at this point in the process is another remarkable strength as it assist to build comprehensive list of low impact risks as the entire impact analysis is being conducted.
According to Kosutic, (2014) the purpose of this analysis is primarily to give one an idea:
a) About the timing of your recovery, and
(b) The timing of your backup, since the timing is crucial – the difference of only a couple of hours could mean life or death for certain organizations if hit by a major incident. For example, if it is a financial institution, recovery time of four hours could mean you will probably survive a disruption, whereas recovery time of 12 hours is unacceptable for certain systems/activities in a bank, and disruption of a full day would probably mean such a bank would never be able to open its doors again. And there is no magic standard which would give you the timing for your organization – not only because the timing for every industry is different, but also because the timing for each of your activities could be different. Therefore, you need to perform the (business) impact analysis to make correct conclusions for likely successful exercise of vulnerabilities.
Hence Business Impact analysis is to evaluate the impact of the affected ICT systems/devices to the business and entire organization which could be loss of integrity, loss of confidentiality or loss of availability.

According to Chia,(2012), CIA refers to Confidentiality, Integrity and Availability as Confidentiality of information, integrity of information and availability of information. Many security measures are designed to protect one or more facets of the CIA triad.
Exercise of vulnerabilities result could result in entire bleach of security goals (***integrity, availability and confidentiality)*** or any of their combinations. Stoneburner et al, explained the security goals in terms of system and data as follows:**.**

a) **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from authorized modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or misleading decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
b) **Loss of Availability**. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.
c) **Loss of Confidentiality.** System and data confidentiality refers to the protection of information

from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

In view of these, magnitude of impact of successful exercise of vulnerabilities could be classified as just ***low or high; high, medium or low*** depending on the risks threshold or appetite of organizations. The classification could also be done along the magnitude of anticipated loss. Finally, this step comes out with impact ratings for probable successful exercise of identified vulnerabilities. Of course, the risk register is consequently updated accordingly and stakeholders are timely communicated of the impact, its ratings and risks under close monitoring (content of the risk register)

Step 7 - Risk Determination
At this step, for the risk to be accurately determined, steps 1 to 6 are put into consideration specifically its respective inputs and outputs. With these, likelihood of vulnerability exploitation, magnitude of the impacts and effectiveness and adequacy of planned and existing controls are thoroughly examined. As output, all the identified risks and associated risk scale (***low, medium or high***). Significant result of this step is the risk matrix which usually 3 x 3(though some organizations may decide to go more granular by adopting 4 x4 or 5 x 5. The matrix is a logical consideration of likelihood of exploitation of the identified vulnerabilities by threat sources and the associated impact if successful which implicitly has considered the existing and planned controls.

Step 8 - Control Recommendations
This is a critical step in the risk assessment process as the consultative and communication channels among stakeholders and the OEMs are further utilized to ensure that commensurate, trendy and best of security controls are recommended to fully mitigate or eliminate existing identified vulnerabilities. With the best of security controls, intending threat sources are totally discouraged or arrested in the course as the costs of successful exploitation of vulnerabilities are made far higher than the anticipated gain thereby discouraging and checking attackers . Hence the output of this step is a list of recommended control in addition to existing controls.

Step 9 - Assessment Documentation and Updating Risk Register
As the final step, all the risk assessment steps and processes are documented including the identified vulnerabilities, impact of successful exploitation, list of existing and recommended controls etc. are presented to the process owners and stakeholders. It is advisable for organizations to create a platform (may be an intranet portal for stakeholders only) on which these reports are timely shared. This is important too, as risk assessment responsibility is for all stakeholders and not "esoterically" reserve for ICT experts as the practice has always been.

IV. Common existing network architecture and its main vulnerabilities

A common typical existing Network architecture is flat and vulnerable as all the data and communication devices such as routers, Idirect, Pixs, switches, fortigate, Pix and many other devices including those from internet Service Providers. These devices are connected directly to the organization`s core switch and/or mostly via the organization`s router. Even the servers, PABX and other telecommunication devices are all connected directly to one and same core switch. Of course, the stacked switches for end users` devices are linked up and also connected to the same core switch.

This design does not only give room for one point of failure(the core switch) for the entire network but any eventual and slightest break-in through any of these devices comfortably drops the attacker into the heart of the organization`s business data and the rest could be story as your guess of the result is as good as mine.

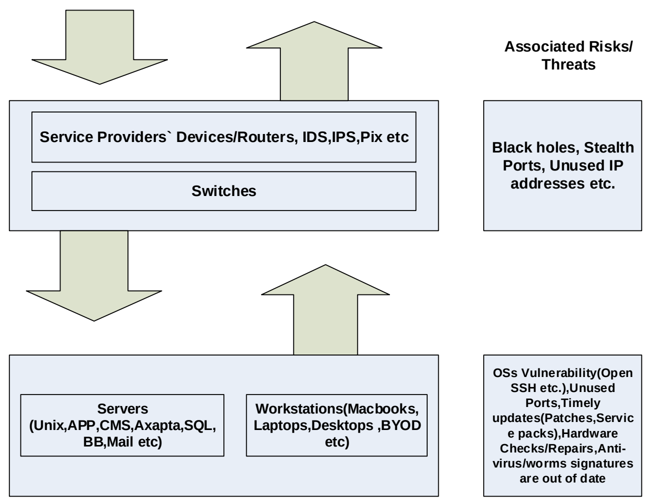

Figure 1: Common Traditional network architecture.

Above block diagram clearly illustrates existing network architecture as implemented by many organizations. The arrows going into the network show traffic from the internet as requested and originated by users in accordance to business needs and the ones going out of the network are traffics sent out by users to fulfill same and/or different business needs.

The first layer shows boundary devices which comprises of the Routers, Idirect, IPS, IDS, Pix, switches and many others as the case may be.

The second layer shows servers(mail,Application,Web server/proxy,DCs,File,Hyper-Vs,DPM,SQL, Axapta,CM etc.), devices such as WAN optimizer,PABX, and end-users` devices such as the laptops, desktops,BYODs etc., of course, its associated risks/threats at the level.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

And most organizations allow remote access such as telnet etc. on the core switch for easy administration of the network from home or out of office, without switch port security, creation of VLANs for the used ports and shutting down unused ports. The risks thereof ranges from Black holes, unused ports, granting access to a range of IP addresses while only few are used,OS vulnerabilities, delayed update of anti-virus and worm signatures etc. This architecture is not a total proof against attacks as a sudden access into any of the boundary devices will totally expose entire network and leaves it at the mercy of the attackers. Again there is no obvious communication and consultation among the stakeholders, not to talk of, with the OEMs

The main Vulnerabilities of the existing network architecture are:

- Being a Flat architecture - all boundary devices are connected to one device and same LAN(no segregation) which makes it easy for an attacker who finds his way into network (router, switch, Idirect, etc.) accidentally or intentionally to fully exercise his attack and bring down the entire network. Also this gives room for one point of total failure for entire network as earlier hinted.
- Granting access to IP address range: If free IP address is sniffed and entrance is successful, routes will be changes and other configurations altered.
- According to Pascucci M.(2012), Router Misconfigurations such as
  - HTTP Open on the core Router: With this, the routes could be changed and NVRAM wiped.
  - Password files stored on Router: Most admins stored company`s credentials on a file on the router`s storage. Most of the routers run SSHv1 and penetration tests gain access to the file which offers limitless access of the company to the invader. Although admins “believe” that .doc cannot be on opened on Cisco IOS.
  - Allow Telnet and other remote accesses open on the boundary devices (routers, switches etc.: Since this is a flat network and telnet is opened to the LAN on the core switch and router, any accidental access to a workstation or even through a compromised user credential via VPN grants an attacker access to the devices which automatically makes it vulnerable.
- According to Manes C. (2014), most common misconfigurations such as:
  - Leaving Shutdown in the remote session options: This is mainly applicable in servers and it’s a common practice by systems/Network administrators and their “reason” being that they want to be able to restart and /or shutdown the device if need be remotely
  - Leaving sample applications and code on a production system: Sample applications are meant to guide you on how to do something .It has been discovered that system administrators inadvertently or intentionally leave both the sample application and codes on the production systems. These are valuable tools for attackers.
  - Autoconfigured IP addresses in DNS: if a server has two ip.addrs in DNS, it will reply to a query with both of them. If one of those addresses is bogus, a client stands a 50:50 chance of trying that bogus address before it tries the legitimate one. This typically means slow performance and call for assistance.
  - Dropping ICMP: This makes it impossible to carry out basic connectivity troubleshooting to the device. However, some administrators drops ICMP which is against the RFCs which states that Hosts must respond to ICMP echo requests. This make it difficult to easily ascertain uptime status of the devices.
  - DNS Islanding in Active Directory (AD): This occurs when a DC points to itself for DNS instead of to another. This makes it, in most cases to be out of synchrony with other DCs and if it stays out for too long (about 60 days default) it simply means that it would not “talk“ to other DCs which makes all the devices that uses it for name resolution will be rendered incommunicado.

V. PROPOSED NETWORK ARCHITECTURE AND ITS RISK PROOF INTEGRATION

The proposed network system architecture has two- layer security which offers proof against all manner of attacks. Figure 4 is a block architecture of the proposed Network Architecture. The two layers are named private and public. The private communication devices boarder the corporate network and are configured with the organization`s Private IP addresses with corresponding subnets such as 10.10.x.x/24. All the corporate communication devices are connected to these devices via stack of Private switches.

However, at the public level, all the connectivity from all service providers` devices are terminated on the public switch on which the public router is directly connected too. The Private router is connected to the public switch. Then the public switch is connected WAN ports of a strong firewall device such as fortigate while its LAN port is connected to the core switch of the LAN.And finally one of the interfaces of the Private router is connected to the same core switch of the LAN. From here (core switch) the signals flow down and up to the stack of private (LAN) switches. However, on the public switch, each connected port has port security access configured and any unused port is shutdown to ensure no vulnerability is

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

exploitable at all. Port security will work on host port. In order to configure port security we need to set it as host port. It could be done easily by switchport mode access command. You can secure trunk connections with port security.

According to Cisco press (2014), the following configuration below illustrates available commands for port security and port shutdown:

To configure port security:
Switch> enable
switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
switch(config)#interface fastethernet 0/1
Switch (config-if)#switchport port-security ?
mac-address Secure mac address
Maximum max secure addressess
<cr>
Switch (config-if)#switchport port-security mac-address ?
H.H.H 48 bit mac address
sticky Configure dynamic secure addresses as sticky
Switch(config-if)#switchport port-security violation ?
protect security violation protect mode
restrict security violation restrict mode
shutdown security violation shutdown mode
Switch(config-if)#switchport port-securityhost

To shutdown a switch port:
Switch> enable
switch#configure terminal
Enter configuration commands,one per line. End with CNTL/Z
Switch (config)# interface gigabitethernet1/0/2

You can verify your settings by entering the show interfaces privileged EXEC command.

In addition to port security, Telnet and other remote accesses are disabled on both the public and private boundary devices. And on the private devices mainly the core switch, the following features are configured:

- Private VLAN edge: This offers security and logical boundary - isolation between ports on a switch, hence ensures that different packets such as the VOIP traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port.

- Port-based ACLs for Layer 2 interfaces: This is security policy applied on per-Layer 2 port basis. With this, incoming traffics are matched against the ACLs and good matches are allowed passage .And others are denied passage.

- Multilevel security on console access: This ensures that only authorized users allowed to effect changes on the configurations of the devices. Hence prevent unauthorized users from altering the switch configurations. Of course, authorized users have varying degree of access which limits what a user can do.

- Granting Specific access on the public layer devices such as to specific host or IP address instead of IP address range or network. This is very critical on this layer. However on the private layer, it can be diluted a little to ensure VLANs talk to one another

- Cisco security VLAN ACLs (VACLs) on all VLANs: This functions as logical boundaries which assures that inhibit unauthorized data flows to be bridged within VLANs.

- Operating Systems Updates: All patches should be tested in a test environment before rolling out to production environment. And whenever in doubt, one of the communication channels (as earlier stated) should be activated and followed-up to ensure timely response.

- Engaging Experts with relevant experience: This is also key to ensure that desired security configurations or intentions are achieved according to organization's needs.

- Port-Level Traffic Controls: This is principally configure on the public layer specifically on the public switch. This offers storm control among many other security features.

  - LAN or network Storm happens when excessive hostile packets are sent continuously on the LAN segment creating unnecessary and excessive traffics which results in network performance degradation. The storm control prevents disruption to regular and normal traffics which is mainly causes by multicast, broadcast or unicast packet storm on any of the physical interfaces.

    To enable traffic storm control feature, at the global configuration mode, use ***storm-control {broadcast | multicast | unicast}.*** However, by default it is disabled. The storm-control action {shutdown |trap} command is used to instruct the switch the action to take when storm is detected. By default, the storm is suppressed which means that no action is configured.

    To verify/check the storm-control suppression levels on an interface, use ***show storm-control [interface] [broadcast | multicast | unicast]*** command.

- Additional Layer 2 best security practices: This is highly recommended to ensure that best of layer 2

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

security measures are in place in the private layer switches(core and other stacked switches).According to Bhaiji Y.(2008),best practice for managing, implementing and maintaining secure layer 2 network are:

- Manage the switches in a secure manner. For example, use SSH, authentication mechanism, access list, and set privilege levels.
- Restrict management access to the switch so that untrusted networks are not able to exploit management interfaces and protocols such as SNMP.
- Always use a dedicated VLAN ID for all trunk ports.
- Be skeptical; avoid using VLAN 1 for anything.
- Disable DTP on all non-trunking access ports.
- Deploy the Port Security feature to prevent unauthorized access from switching ports.
- Use the Private VLAN feature where applicable to segregate network traffic at Layer 2.
- Use MD5 authentication where applicable.
- Disable CDP where possible.
- Prevent denial-of-service attacks and other exploitation by disabling unused services and protocols.
- Shut down or disable all unused ports on the switch, and put them in a VLAN that is not used for normal operations.
- Use port security mechanisms to provide protection against a MAC flooding attack.
- Use port-level security features such as DHCP Snooping, IP Source Guard, and ARP security where applicable.
- Enable Spanning Tree Protocol features (for example, BPDU Guard, Loopguard, and Root Guard).
- Use Switch IOS ACLs and Wire-speed ACLs to filter undesirable traffic (IP and non-

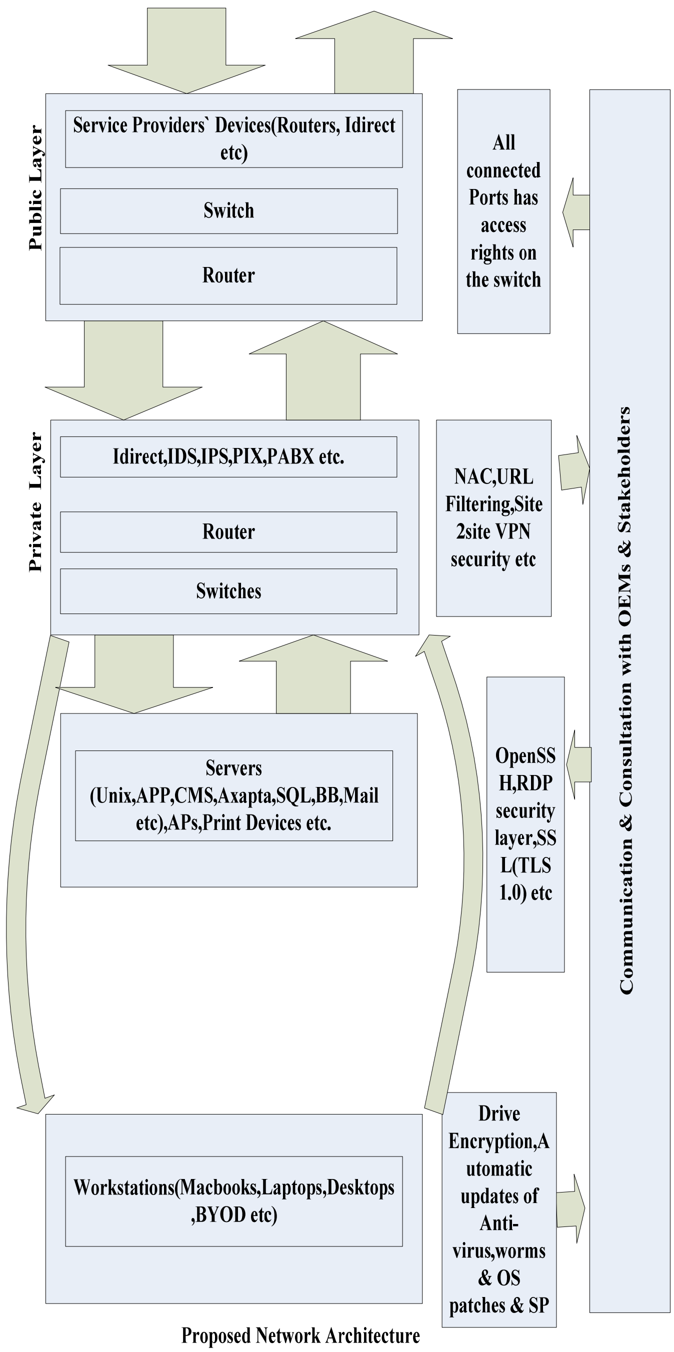

Figure 2: Proposed Layered Network architecture using data and communication devices

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

This totally eliminates possible entrance of the intentional or accidental attackers/invader. And this drives steady communication and consultation among stakeholders/OEMs to ensure that Operating systems of the devices are always updated both on the private, public and entire corporate network. In addition, necessary advance security measures are implemented at appropriate layers.

With steady communication and consultation of OEMs, the stakeholders are provided with updates,firmwares, patches or service packs and some customized net scanners such as Microsoft Baseline Security Analyzer(MBSA) for windows platform and Open Vulnerability Assessment System(OpenVAS) for open-source related (Cisco,Avaya,android etc.) Platform. These customized applications detect common security misconfigurations and vulnerabilities in the data and communication devices. And with these scanners, organizations can frequently carry our in-depth checks for vulnerabilities and any low priority ones such as patches, OS updates etc. detected are added to the risk register for close watch and monitoring.

The result from this, forms further basis for thorough risk assessment on all the layers of devices to ensure the targeted integrity, availability and confidentiality

VI. CONCLUSION

Every Organization has mission and vision which is backed and driven by strong information and communication technology. And due to ever dynamic and unique nature of information and communication technology, data and communication devices cannot move out way of trouble. In fact, they are more vulnerable to economic and political uncertainties than any other investments. In view of this, above proposed network architecture is key, to ensure that organizations are proactively positioned to eliminate inherent vulnerabilities of common network architecture and take advantage of the proposed solutions.

Furthermore, since attacks assume dynamic forms, it is advisable to charge network Engineers , systems administrators and Experts to make this process a daily routine and carry out aggressive end-users awareness campaign on what to do once they sense data compromise vis-à-vis Integrity, Availability and confidentiality. This is important as Risk assessment is the duty of all stakeholders hence the encouragement to ensure consistent two-way communication and consultation among stakeholders.

VII. REFERENCE

[1] Stoneburner G., Goguen, A. & Feringa, A. (2002). Risk Management Guide for Information Systems. Retrieved January 4, 2015 From http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[2] Alshboul, A. (2010).Information Systems Security measures and countermeasures: Protecting Organizational Assets from malicious Attacks, 3, Article 486878. Journals on Communications of the IBIMA, 2010, 1-9. Retrieved March 15 2015 from http://www.ibimapublishing.com/journals/CIBIMA/2010/486878/486878.pdfJ.

[3] Bhaiji, Y.(2008). Security Features on Switches(courtesy Csico press). Retrieved on December 7, 2017 from http://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=3

[4] Chia, T., (2012). Confidentiality, Integrity, Availability: The three components of the CIA Triad. http://security.blogoverflow.com/2012/08/ Confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

[5] Manes C.(2014). The 21 most common misconfigurations that will come back to haunt you!Retrieved March 20 2015 from http://www.gfi.com/blog/the-21-most-common-misconfigurations-that-will-come-back-to-haunt-you/

[6] Kosutic, D., (2014). Risk Assessment vs. Business Impact Analysis. http://webcache.googleusercontent.com/search?q=cache: 8eF68VJu0cYJ: advisera.com/27001academy/knowledgebase/risk-assessment-vs-business-impact-analysis/+&cd=1&hl=en&ct=clnk&gl=ng

[7] Pascucci M.(2012).Network Security Horror Stories: Router Misconfigurations.Retrieved March 22 2015 from http://blog.algosec.com/2012/09/network-security-horror-stories-router-misconfigurations.html

[8] IRS Office of Safeguards Technical Assistance Memorandum Protecting Federal Tax Information (FTI) Through Network Defense-in-Depth. Retrived April 20, 2015 from https://www.irs.gov/pub/irs-utl/protecting-fti-throughnetworkdefense-in-depth.doc.

[9] Cisco Press(2014). Cisco Networking Academy's Introduction to Basic Switching Concepts and Configuration .